IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 09/852,336

Inventors: James Duncan Work

Filed: 5/8/2001

Art Unit: 2153

Examiner: Chea, Philip J.

Confirmation No.: 4814

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This revised Brief is submitted in response to the Notification of Non-Compliant Appeal Brief mailed October 29, 2007. Consideration of this appeal by the Board of Patent Appeals and Interferences for allowance of the above-captioned patent application is respectfully requested.

Table of Contents

I.   REAL PARTY IN INTEREST

The real party in interest is LinkedIn Corporation, a corporation of Delaware having a place of business at 1840 Embarcadero Road, Palo Alto, CA 94303.

II.   RELATED APPEALS AND INTERFERENCES

This application has not previously been the subject of an appeal or interference proceeding.

III.   STATUS OF CLAIMS

Claims 1-147, 153, 154, 157, 159, 160 and 163-171 have been cancelled. Claims 148-152, 155, 156, 158, 161, 162 and 172-178 are currently pending, have been finally rejected, and are the subject of this appeal.

IV.   STATUS OF AMENDMENTS

There are no currently pending amendments.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

Claim 148 reads as follows:[1]

> 148. A computer-implemented method, comprising reporting matches
> to searches [70] initiated by a searcher so long as access control criteria
> [24, 36] are met, the matches including potential targets satisfying one
> or more search criteria defined for the searches, and the access control
> criteria (i) being selectably controllable by any of one or more persons
> in one or more chains of person-to-person relationships connecting and
> including the searcher and the potential targets, and (ii) defining ranked
> access levels [64] assigned to said one or more persons, said access
> levels being defined in terms of attributes of relationships that exist
> between any two persons in each of said chains of person-to-person
> relationships connecting the searcher and the potential target to which
> each of the matches pertain.

As indicated by this claim, the present invention relates to a method of,

> (i) reporting matches (e.g., potential targets) to searches initiated by a
>
> searcher (see, e.g., Specification at ¶ 44, describing a personal search agent),
>
> when certain search criteria and access control criteria are satisfied. See, e.g.,

---

[1] Reference numbers as used in the drawings have been inserted in accordance with 37 C.F.R. § 41.37(c)(1)(v). Such reference numbers are shown in brackets "[ ]" to distinguish them from the Roman numeral numbering scheme used in the claim. The use of such reference numbers should in no way be read as limiting the claim to the illustrated embodiment.

Specification at ¶ 44 and 46, describing search process and maintenance of privacy; ¶¶ 63-64, describing the use of personal access controls that put control over access to personal information; etc. (i.e., restricting search results in accordance with user-specified conditions). See especially page 31, line 5 - page 32, line 4; ¶ 80, page 37, lines 11-14; ¶ 82, page 38, lines 4-7 ("the network broker agent 38 can access confidential information regarding system users and/or their contacts and use it to make highly accurate matches, but will only reveal the information when given permission by each user's personal access or access agent 24."), and lines 7-10, discussing a search being performed in such a manner as to assess whether a particular user's profile satisfies one or more search criteria specified by the searcher. And see Specification at ¶¶ 106 and 111, describing the reporting of matches to search criteria.

(ii) wherein the access control criteria are selectably controllable by any of one or more persons in one or more chains of person-to-person relationships connecting and including the searcher and the potential targets. See, e.g., Specification at ¶ 64 (users having control over release of access to profile information); ¶ 79 (user control access rights through profile builder); ¶ 82, page 38, lines 10-16, (network broker agent only reveals information when given permission by each user's personal access or access agent) ¶ 83, page 38, lines 17-18 (use of trusted referral relationships); and ¶ 109 (access is granted according to access control restrictions specified by user).

(iii) the access control criteria define ranked access levels assigned to these one or more persons. See Specification at ¶¶ 65 ("The system of security values is matched by a method of applying access codes to individuals, organizations, or groups defined by customizable sets of criteria.", 68-72 (describing different sets of access rights ranked according to degree of access, type of relationship to user, and system-only access); and 81 (server-side agent duplicates client-side agent).

(iv) and the access control criteria are defined in terms of attributes of relationships that exist between any two of those persons forming the chain of person-to-person relationships. See e.g., Specification at ¶ 69 access rights defined in terms of relationships to users), ¶73 ("security settings are defined by either simple or complex rules relating to elements in people's profiles, and to the indicators that users select to indicate their relationship to their contacts and to other people who may or may not yet have a profile in the system"); ¶ 82, page 38, lines 10-16, ¶ 83, page 38, lines 17-18, ¶ 103, page 47, lines 6-19; and ¶ 110 (trusted paths determined through user connections).

Claim 172 reads as follows:

> 172. A computer-implemented method, comprising reporting matches
> [70] to search criteria specified in a search initiated by a searcher so
> long as a connection strength [64] between each two people forming a
> person-to-person connection in a chain of person-to-person connections
> between the searcher and a potential target exceeds a connection
> strength threshold, said connection strength being an attribute of access
> control criteria [24, 36] that are selectably controllable by any of one
> or more persons in said chain of person-to-person connections between
> the searcher and the potential target.

As indicated by this claim, the present invention relates to a method for reporting matches when each group of two persons, forming a chain of person-to-person connections between the searcher and a potential target, has a connection strength exceeding a connection strength threshold. The connection strength is an attribute of access control criteria that is selectably controllable by any person in the chain connecting the searcher and the target. For example, paragraph [0107] of Applicant's specification states:

> To perform the search, the broker agent 38 parses the search request
> into component parameters thereof and conducts a search in the
> User_Profiles portion of database 42 to try to find best matches. If the
> search parameters include connection types and weights, then the
> broker agent 38 will seek connection paths that match the connection
> parameters. This may include strategies such as: starting with targets
> and working backward to try to connect to the searcher, via likely
> connectors; or starting with the searcher's contacts and working
> outward to try to connect to targets or other likely connectors.
> Searching proceeds to the levels defined by the search extents entered
> by the user (or to a default level if none were entered).

The Specification describes the process of reporting matches to searches initiated by a searcher when certain search criteria and access control criteria are satisfied. See, e.g., Specification at ¶ 44 and 46, describing search process and maintenance of privacy; ¶¶ 63-64, describing the use of personal access controls that put control over access to personal information; etc. (i.e., restricting search results in accordance with user-specified conditions). See especially page 31, line 5 - page 32, line 4; ¶ 80, page 37, lines 11-14; ¶ 82, page 38, lines 4-7 ("the network broker agent 38 can access confidential information regarding system users and/or their contacts and use it to make highly accurate matches, but will only reveal the information when given permission by each user's personal access or access agent 24."), and lines 7-10, discussing a search being performed in such a manner as to assess whether a particular user's profile satisfies one or more search criteria specified by the searcher. And see Specification at ¶¶ 106 and 111, describing the reporting of matches to search criteria.

The concept of access control criteria that are selectably controllable by any of one or more persons in one or more chains of person-to-person relationships connecting and including the searcher and the potential targets is described in the Specification, for example, at ¶ 64 (users having control over release

of access to profile information); ¶ 79 (user control access rights through profile builder); ¶ 82, page 38, lines 10-16; (network broker agent only reveals information when given permission by each user's personal access or access agent); ¶ 83, page 38, lines 17-18 (use of trusted referral relationships); and ¶ 109 (access is granted according to access control restrictions specified by user). One of these access control criteria is a connections strength. See, e.g., specification at ¶ 13 (search criteria may include portions of descriptive profiles of the potential targets, which profiles may include indications of the nature and strength of the relationship of the searcher to the target and/or to the target's organization); ¶ 55 (a profile builder allows users to describe their relationships to their contacts and the relationships of contacts to one another); ¶ 82 (if the search parameters specify connection criteria, such as level of trust, type of connection, etc., then the network broker can discover and evaluate connection paths between the searcher and the prospective target on those parameters).

The access control criteria are defined in terms of attributes of relationships that exist between any two of those persons forming the chain of person-to-person relationships. See e.g., Specification at ¶ 69 access rights defined in terms of relationships to users); ¶73 ("security settings are defined by either simple or complex rules relating to elements in people's profiles, and to the indicators that users select to indicate their relationship to their contacts and to other people who may or may not yet have a profile in the system"); ¶ 82, page 38, lines 10-16, ¶ 83, page 38, lines 17-18, ¶ 103, page 47, lines 6-19; and ¶ 110 (trusted paths determined through user connections).

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1) Claims 148, 150, 155-156, 158, 172, 174, and 177-178 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Michalski ("Collaborative Filters").

2) Claims 149, 173 and 175-176 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Michalski ("Collaborative Filters") in view of the general level of skill in the art.

3) Claims 151-152 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Michalski ("Collaborative Filters") in view of Kantz et al. ("The Hidden Web").

4) Claims 161-162 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Michalski ("Collaborative Filters") in view of Walker et al., U.S. Patent No. 5,884,270.

VII.   ARGUMENT

1.   *Claims 148, 150, 155-156, 158, 172, 174 and 177-178 are not anticipated by the Michalski reference ("Collaborative Filters") under 35 U.S.C. § 102(b).*

The Michalski reference is not an enabling disclosure with respect to each and every limitation of the claims, as a group.

In order for a reference to qualify as anticipatory prior art, the reference must include an enabling disclosure. That is, the reference must describe how to make and how to use the invention. The disclosure in an assertedly anticipating reference must provide an enabling disclosure of the desired subject matter; mere naming or description of the subject matter is insufficient, if it cannot be produced without undue experimentation. *Elan Pharm., Inc. v. Mayo Found. For Med. Educ. & Research*, 346 F.3d 1051, 1054, 68 USPQ2d 1373, 1376 (Fed. Cir. 2003).

The Michalski reference is not enabling because it fails to describe how to make and how to use the invention as claimed. Rather, the Michalski reference describes various desirable features. For example, paragraph one on page fifteen of Michalski states, "[the system] *would also have to offer* various levels of participation and trust, to help people distinguish a likely connection (you should meet him) from a recommendation (you should trust everything he says)." In this case, the Michalski reference suggests various levels of participation and trust are desirable *features*, but does not describe *how* the features are implemented and/or used.

Similarly, paragraph five on page fifteen of Michalski states, "[p]ersonal gatekeeper agents are able to give access at varying levels of security, based on levels of trust." The Michalski reference does not describe how the "levels of trust" are implemented and used. For instance, the Michalski reference does not indicate who determines and sets the "levels of trust." Furthermore, the Michalski reference does not indicate what information or attributes the "trust levels" apply to.

The Michalski reference describes what can best be considered aspirational goals for Mr. Work, but does not describe how the problems he is addressing can actually be solved. Recognizing a problem does not define an invention and stating a problem does not anticipate one. Instead, it is solving a problem that defines when an invention has been made and it is communication of the solution which is required to anticipate same. At best, the Michalski reference can be said to have noted several problems faced by those in the field of the invention, but only the present application (and not the cited reference) describes how those problems were overcome to arrive at the claimed invention. Furthermore, the Examiner appears to be employing hindsight analysis and reading into the Michalski reference more than is actually there.

The Michalski reference's lack of enablement is further evidenced in the text of the Michalski reference itself, which essentially states at paragraph seven on page fifteen that the system being described is a work-in-progress, with many features not yet worked out or implemented:

> There are aspects of identity management that Work has yet to solve, as
> well as projects outside his immediate view that he has not yet drawn
> on.

Consequently, Applicant submits that the Examiner's rejection of claims 148, 150, 155-156, 158, 172, 174 and 177-178 under 35 U.S.C. § 102(b) cannot be properly upheld. Allowance of the claims is requested.

Independent claim 148 in particular is not anticipated by the Michalski reference, because the Michalski reference fails to describe reporting matches based on chains of person-to-person relationships.

The Michalski reference is a report about systems that use collaborative filters. As described in paragraph five on page two of the Michalski reference, collaborative filters are a subset of systems for making recommendations, for example, by collecting user ratings of items in a domain, and then using the ratings to offer recommendations of other items in the domain. The most relevant passage in the Michalski reference (page fifteen) describes a system in which the domain is people, and users of the system essentially rate or rank people in some fashion. However, there is nothing in the Michalski reference describing a system in which matches are reported based *on chains of person-to-person relationships* that are established between the searcher and a target. Furthermore, in the context of collaborative filtering, the term "level of trust" may imply a rating, but it does not imply that there need be a personal relationship between the person doing the rating and the person being rated.

Specifically, claim 148 states that a match is reported when access control criteria are met, wherein the access control criteria are "selectably controllable by any of one or more persons *in one or more chains of person-to-person relationships connecting and including the searcher and the potential targets*." Accordingly, chains of person-to-person relationships are formed, in part based upon access control criteria that are established by each person forming a link in the chain of person-to-person relationships. Thus, despite search criteria being met, where a link between two people would be established but for satisfying access control criteria, no chain connecting the searcher and the target may exist. Consequently, by setting access control criteria, each person in a potential chain of persons connecting the searcher and a target has a say in whether such a chain can be formed. The Examiner has suggested this aspect of the claimed invention is disclosed in paragraph one on page fifteen of the Michalski reference, which states:

> All the systems we have examined so far feature people rating inert
> items such as tunes, movies or books. What if one turned that attention
> on other people? Of course, most people aren't inert, so the system
> would have to provide both safeguards against inappropriate use of
> information and incentives for participating and offering information.
> More than that, it would also have to offer various levels of
> participation and trust, to help people distinguish a likely connection
> (you should meet him) from a recommendation (you should trust

everything he says). That's the ambitious system that Duncan Work is designing

Applicant submits that the passage cited by the Examiner does not disclose or suggest access control criteria "selectably controllable by any of one or more persons *in one or more chains of person-to-person relationships connecting and including the searcher and the potential targets*." Moreover, the Michalski reference does not describe a system in which chains of person-to-person relationships are formed.

Paragraph six of page fifteen of the Michalski reference states "[the system] helps link informal networks of people " However, the term "informal networks of people" is not defined, nor is there an explanation or description of *how* this is implemented or achieved. That is, the Michalski reference does not disclose and enable the claimed invention. Specifically, there is no mention of access control criteria "selectably controllable by any of one or more persons *in one or more chains of person-to-person relationships connecting and including the searcher and the potential targets*." Accordingly, Applicant submits that Michalski does not anticipate independent claim 148. For the same reasons, dependent claims 149-152, 156, 158, 161, 162, and 176-178, which depend directly or indirectly upon claim 148, are also not anticipated by the Michalski reference. Allowance of these claims is requested.

Independent claim 172 is not anticipated by the Michalski reference, because the Michalski reference fails to describe a connection strength between each two people forming a person-to-person connection in a chain of person-to-person connections exceeding a connection threshold.

Claim 172 states that matches to a search are reported when "a connection strength between each two people forming a person-to-person connection in a chain of person-to-person connections between the searcher and a potential target exceeds a connection strength threshold." The Michalski reference does not disclose or suggest the above feature. The Examiner has suggested that the above features are disclosed at paragraph five of page fifteen of the Michalski reference, which states

> If Work can build a user community with the right mix of incentives and trust, Net Deva promises to offer an environment in which people can share information normally considered too personal to offer to others, including people's capabilities, professional relationships, goals and values. Personal information is available to the network broker, but not to individuals, unless it is specifically allowed by the guarding gatekeeper. Personal gatekeeper agents are able to give access at varying levels of security, based on levels of trust.

Applicant submits that the above passage does not disclose or suggest the concept of a connection strength, as claimed in claim 172. In general, the above passage relates to sharing personal information. However, there is nothing in the passage above, or in the Michalski reference, disclosing or suggesting reporting matches based on *connection strengths between persons forming a chain of person-to-person connections*.

Paragraph four of page fifteen of the Michalski reference states, "[t]he gatekeeper agents manage information access by evaluating the relevance of requests for communication and checking the validity and trust levels of the agents making the requests." Moreover, as described above, the term "trust levels" has not been defined in the Michalski reference. A trust level is not the same as a connection strength or a connection strength threshold, as claimed in claim 172. To the extent that a level of trust or trust level is similar to a connection strength, the Michalski reference does not disclose or suggest that matches are reported when a trust level (or connection strength) between each two people forming a person-to-person connection in a chain of person-to-person connections between the searcher and a potential target exceeds a threshold (i.e. a connection strength threshold). As stated above, Michalski is not an enabling disclosure, particularly with respect to independent claim 172.

For at least the reasons stated above, claim 172 is not anticipated by the Michalski reference. Similarly, claims 173-175, which depend directly upon claim 172, are not anticipated by Michalski. Accordingly, Applicant respectfully requests allowance of the claims.

2.   *Claims 149, 173, 175-176 are not obvious under 35 U.S.C. § 103(a) in view of Michalski.*

The Examiner rejected dependent claims 149, 173, and 175-176 as being obvious under 35 U.S.C. § 103(a) in light of Michalski ("Collaborative Filters"). In support of the rejection, the Examiner simply states that one skilled in the art would find it obvious to include features claimed by the Applicant in the system described by Michalski.

With respect to claims 149 and 175, the Examiner readily admits that Michalski does not disclose search criteria that define a minimum connection strength for a person-to-person relationship that is required between persons forming said one or more chains of person-to-person relationships connecting the searcher and the potential targets. However, the Examiner relies on Michalski and simply states that one skilled in the art would have found it obvious to include such a feature in the system described by Michalski. Similarly, no evidence is provided or suggested by the Examiner in rejecting claims 173 and 176. The Examiner simply states the claims would be obvious to one skilled in the art.

First, as claims 149, 173, 175-176 are dependent claims, the arguments above with respect to claims 148 and 172 are applicable here as well. That is, dependent claims 149, 173, 175-176 are not anticipated or obvious in view of Michalski for the reasons set out above. Furthermore, with the exception of the Michalski reference, the Examiner provides no evidence whatsoever to support the rejection of claims 149, 173, 175-176 under 35 U.S.C. § 103(a). A rejection under 103(a) is improper and should not be upheld when the rejection simply states that one skilled in the art would find a particular claim limitation obvious. For the reasons herein, Applicants submit that claims 149, 173, 175-176 are not obvious in view of Michalski and the level of skill in the art.

3. **Claims 151 and 152 are not obvious under 35 U.S.C. § 103(a) in view of Michalski and Kautz et al. ("The Hidden Web").**

The Examiner has rejected claims 151 and 152 as allegedly being obvious under 35 U.S.C. § 103(a) in view of a combination of Michalski and Kautz et al. ("The Hidden Web").

Dependent claim 151 is not obvious in view of the combination of the Michalski reference and the Kautz reference.

Dependent claim 151, which is dependent upon claim 148, is not obvious in view of Michalski and Kautz for the reasons stated above with respect to independent claim 148. Specifically, Applicant submits that neither reference discloses or suggests access control criteria "selectably controllable by any of one or more persons *in one or more chains of person-to-person relationships connecting and including the searcher and the potential targets.*"

Dependent claim 152 is not obvious in view of the combination of the Michalski reference and the Kautz reference.

As with claim 151, dependent claim 152 is not obvious in view of Michalski and Kautz for the reasons stated above with respect to independent claim 148. Specifically, Applicant submits that neither reference discloses or suggests access control criteria "selectably controllable by any of one or more persons *in one or more chains of person-to-person relationships connecting and including the searcher and the potential targets.*" Moreover, neither Michalski nor Kautz disclose or suggest a connection threshold that is part of access control criteria selectably controllable by any persons in a chain of person-to-person relationships forming a chain connection the searcher and the target. For instance, consistent with claim 152, any person in a potential chain of persons connecting a searcher and a target can control whether such chain is formed by establishing a connection threshold indicating a maximum number of person-to-person relationships to be allowed in establishing said one or more chains of person-to-person relationships. In contrast, the Kautz reference shows a setting for a search which controls the depth of a chain only for purposes of the search. Kautz does not disclose or suggest that any person that might form a chain has control over whether such a chain is actually formed. In short, Kautz does not disclose the limitation of dependent claim 152.

4. **Claims 161 and 162 are not obvious under 35 U.S.C. § 103(a) in view of Michalski and U.S. Patent No. 5,884,20 to Walker et al.**

Dependent claims 161 and 162 are dependent upon claim 148. For the reasons stated above in connection with claim 148, dependent claims 161 and 162 are not obvious in view of Michalski and Walker. Specifically, Walker does not disclose any of the limitations referenced above in connection with claim 148, and therefore, even the additional disclosure of Walker does not render claims 161 and 162 obvious.

For at least the foregoing reasons, the claims are patentable over the references cited in the Office Action. If there are any additional fees due in connection with this communication, please charge our deposit account no. 19-3140.

Respectfully submitted,

SONNENSCHEIN NATH & ROSENTHAL LLP

Dated: <u>December 31, 2007</u>

<u>/Tarek N. Fahmi/</u>
Tarek N. Fahmi
Reg. No. 41,402

P.O. Box 061080
Wacker Drive Station
Sears Tower
Chicago, IL 60606-1080
(650) 798-0300

The claims on appeal read as follows:

1-147. (Canceled).

148.   (Previously Presented) A computer-implemented method, comprising reporting matches to searches initiated by a searcher so long as access control criteria are met, the matches including potential targets satisfying one or more search criteria defined for the searches, and the access control criteria (i) being selectably controllable by any of one or more persons in one or more chains of person-to-person relationships connecting and including the searcher and the potential targets, and (ii) defining ranked access levels assigned to said one or more persons, said access levels being defined in terms of attributes of relationships that exist between any two persons in each of said chains of person-to-person relationships connecting the searcher and the potential target to which each of the matches pertain.

149.   (Previously Presented) The computer-implemented method of claim 148, wherein one attribute includes connection strengths for person-to-person relationships and wherein said search criteria define a minimum connection strength for a person-to-person relationship that is required between persons forming said one or more chains of person-to-person relationships connecting the searcher and the potential targets.

150.   (Previously Presented) The computer-implemented method of claim 148, wherein at least one attribute comprises an indication of a connection strength for at least one of the person-to-person relationships between persons forming said one or more chains of person-to-person relationships.

151.   (Previously Presented) The computer-implemented method of claim 148, wherein the search criteria include a connection threshold specified by the searcher, the connection threshold indicating a maximum number of person-to-person relationships to be allowed in establishing said one or more chains of person-to-person relationships connecting the searcher and the potential targets.

152.   (Previously Presented) The computer-implemented method of claim 148, wherein the access control criteria comprise a connection threshold indicating a maximum number of person-to-person relationships to be allowed in establishing said one or more chains of person-to-person relationships.

153.   (Cancelled)

154.   (Cancelled)

155.   (Previously Presented) The computer-implemented method of claim 148, wherein the matches are reported only so long as a connection between each person associated with said one or more chains of

person-to-person relationships connecting the searcher and the potential targets satisfies at least one attribute of the access control criteria established by a next subsequent connector in a connection path between the searcher and the potential target.

156.   (Previously Presented) The computer-implemented method of claim 148, wherein reporting matches to searches initiated by a searcher so long as access control criteria are met further comprises autonomously brokering connections between the searcher and the potential target so as to provide information regarding the one or more persons in the one or more chains of person-to-person relationships connecting the searcher and the potential targets.

157.   (Cancelled)

158.   (Previously Presented) The computer-implemented method of claim 156, wherein autonomously brokering connections between the searcher and the potential target further comprises brokering, in accordance with one or more instructions supplied by any one or more connecting individuals in an inter-personal connection path from the searcher to a potential target, where such instructions refer to one or more of said attributes of relationships between any two or more said persons in said chains.

159.   (Cancelled)

160.   (Cancelled)

161.   (Previously Presented) The computer-implemented method of claim 148, wherein one attribute determines whether a third party evaluation report is accessible to the searcher, said third party evaluation report (i) pertaining to a person forming a person-to-person relationship connecting the searcher and the potential target, and (ii) being integrated with a personal profile of said person forming a person-to-person relationship connecting the searcher and the potential target.

162.   (Previously Presented) The computer-implemented method of claim 161, wherein said third party evaluation report is not accessible to said person forming a person-to-person relationship connecting the searcher and the potential target.

163.   (Cancelled)

164.   (Cancelled)

165.   (Cancelled)

166.   (Cancelled)

167.   (Cancelled)

168.   (Cancelled)

169.   (Cancelled)

170.   (Cancelled)

171.   (Cancelled)

172.   (Previously Presented) A computer-implemented method, comprising reporting matches to search criteria specified in a search initiated by a searcher so long as a connection strength between each two people forming a person-to-person connection in a chain of person-to-person connections between the searcher and a potential target exceeds a connection strength threshold, said connection strength being an attribute of access control criteria that are selectably controllable by any of one or more persons in said chain of person-to-person connections between the searcher and the potential target.

173.   (Previously Presented) The computer-implemented method of claim 172, wherein the connection strength threshold is included in the search criteria specified by the searcher.

174.   (Previously Presented) The computer-implemented method of claim 172, wherein the connection strength threshold is established by the potential target.

175.   (Previously Presented) The computer-implemented method of claim 172, wherein the connection strength threshold determines the minimum connection strength required between two people forming a person-to-person connection in a chain of person-to-person connections between the searcher and the potential target.

176.   (Original) The computer-implemented method of claim 148, wherein said relationships include a relationship to a group with which at least one of said persons in one of said chains is associated.

177.   (Original) The computer-implemented method of claim 148, wherein said access levels are autonomously derived and assigned based on instructions provided by said persons, said instructions referring to combinations of said attributes of relationships.

178.   (Original) The computer-implemented method of claim 148, wherein said access levels are autonomously derived and assigned based on data about said attributes of relationships.

Evidence Appendix:
(37 C.F.R. § 41.37(c)(1)(ix))

There is no evidence submitted under 37 CFR 1.130, 1.131 or 1.132, or other evidence entered by the examiner and relied upon by the appellant in this appeal.

Related Proceedings Appendix:
(37 C.F.R. § 41.37(c)(1)(x))

There are no related proceedings to report.